Data Privacy and Confidentiality in The Public Arena

Mary Etta Mills, ScD, RN, CNAA
Department of Education, Administration,
Health Policy and Informatics
University of Maryland School of Nursing
Baltimore, Maryland

Public policy debates concerning the collection of healthcare information for use as aggregate databases to underpin healthcare planning are growing increasingly rankerous. Provider concerns for future patient relationships and public fear of damages resulting from information disclosure are driving the development of data collection policy. Through a special Task Force, the State of Maryland has addressed these issues and developed policy recommendations specific to data collection and use.

INTRODUCTION

The creation of a national network for sharing and storing patients' medical information in a standardized form has been one goal of health care legislation. At present, 35 states collect hospital service data, 17 states collect outpatient data and 4 states collect physician data.

In 1995, the State of Maryland began the development of a specialized medical care database to compile statewide data on health services rendered by health care practitioners and office facilities. Through state regulation the Health Care Access and Cost Commission was directed to submit reports to the Maryland General Assembly describing the cost and utilization of health care services in Maryland, provide per capita health care expenditure information, support private and public purchasers' efforts to identify cost-effective practitioners, enable providers to assess the productivity of their practices and assist in the development of a practitioner payment system for the State of Maryland.

To prepare for these efforts and assure the public interest would be met with regard to privacy concerns, a study was initiated of privacy and confidentiality issues that would surface if patient-specific information was required as part of the database.

METHOD

The Maryland Health Care Access and Cost Commission appointed a Privacy and Confidentiality Workgroup to hold public debates on each of six key issues. These issues centered on the effect of data collection on self-pay patients, use of unique patient identifiers, access to personally identifiable data, protections for proprietary information, development of public use data, and third party access to other then public-use data sets.

Source of Issues

These issues were especially important since, by regulation, the medical care data base was structured to collect for each type of patient encounter with a health care practitioner or office facility, information which included: patient demographic characteristics; principle diagnosis; procedure performed; date and location of where the procedure was performed; the charge for the procedure; whether the bill for the procedure was submitted on an assigned or nonassigned basis; a health care practitioner's universal identification number; prescription drugs for each type of patient encounter with a pharmacist; and, information relating to health care costs, utilization, or resources from payors and governmental agencies.

Forum Structure

The Workgroup was composed of sixteen members who represented the parent commission and two other Statewide commissions- the Maryland Health Resources Planning Commission and the Maryland Health Services Cost Review Commission- plus representatives from the Psychiatric Association, Federal Confidentiality Task Force, the Department of Health and Mental Hygiene, the Maryland HMO Association, Medical-Legal Community, AIDS Legislative Action Committee, Consumers, Ethicist, Mental Health Affiliation, and AFL-CIO. Public notice was given of all meetings and discussion was facilitated over a twenty month period extending from July, 1995 to February, 1997.

1091—8280/97/$5.00

Definitions
Specific reference to "health care practitioner" included anyone who is licensed, certified or otherwise authorized under the Health Occupations Article to provide health care services. "Health care service" meant any health or medical care procedure or service rendered by a health care provider that provides testing, diagnosis, or treatment of human disease or dysfunction; or, dispenses drugs, medical devices, medical appliances, or medical goods for the treatment of human disease or dysfunction. Finally, "office facility" included any free standing facility providing ambulatory surgery, radiological or diagnostic imagery or laboratory services.

CONSIDERATIONS

Privacy and Confidentiality Law
Courts have worked diligently to define the "zone of privacy" that the Constitution protects. Although the interests embodied in the right to privacy are multi-faceted, in the context of government data collection efforts, two recognized privacy interests are involved. "One is the individual interest in avoiding disclosure of personal matters and another is the interest in independence in making certain kinds of important decisions."[1] Case law has been used to show the interplay between state law and constitutional privacy rights. While there is a general recognition that a patient has a right to privacy in medical records, that right is not absolute. "The individual privacy interest in the patient's medical records must be balanced against the legitimate interests of the state in securing the information contained therein."[2] Many courts adopt an analytical structure employed by the Third Circuit United States Court of Appeals which specifies several factors to consider in weighing competing interests such as the type of record requested, the information it contains, the potential for harm in subsequent disclosure, the adequacy of safeguards to prevent unauthorized disclosure, the government's need for access, and whether there is an express statutory mandate towards access.

Different from the constitutional right to privacy is the assurance of medical record confidentiality made by statute. Although the right to privacy may give way to the government's need for information, the statutory mandates of confidentiality must be adhered to. For example, these statutes may provide for limits on the disclosure of all patient medical records and may govern access to specific disease records, as well as make disclosures of some treatment records (e.g. alcohol and drug abuse) subject to federal laws and regulations.

For policy considerations, privacy refers to how the individual can control their individual information. Confidentiality is the totality of the rules that govern how information is to be used and security is how information and the systems that contain it are protected.

ISSUES AND RECOMMENDATIONS

Self Pay
Consideration of data collection of all health care encounters regardless of payment source surfaced a concern for the potentially negative impact on consumers who choose to seek care outside of their regular health care plans in order to protect what they believe to be potentially damaging information. Of special concern, were individuals seeking mental health services.

In a survey of certain practitioners in Maryland to ascertain self-pay statistics, psychiatrists indicated that 48% of their patient visits were paid directly by the patient. The reasons for this high rate of self pay included concerns for privacy, coverage issues and differences in the business practices of psychiatrists. These findings were supported by the 1993 Harris/Equifax Health Care Privacy Survey which revealed that 75 per cent of the public worry that medical information (not specific to mental health) from a computerized health information system will be used for many non-health purposes.[3]

The initial logic of full data collection anticipated that if some patients were allowed to "opt out" of the system, others would also choose this option and the data base would be less accurate for purposes of analysis.

After lengthy debate, compelling arguments were made for "individual liberty versus the authority of governments," concern that data security could not be absolutely guaranteed, and implications of consumers taking a "no treatment option." As a result, legislation was passed at the State level that precluded the collection of self-pay encounters and limited the use of the payer-supplied encrypted identifiers.

Unique Patient Identifiers
Connected to the self pay issue was the onus to have

clear protections for all data. This included the consideration of unique patient identifiers. In order to be a unique identifier, requirements included: uniqueness; reliability; accessibility (recovery if lost);and brevity. Frequently the social security number is selected as a unique identifier but this was considered neither secure nor reliable. Current identifiers are problematic in that patients may have several "health care" identifiers, legally use several names; and legally use several social security numbers, and addresses.

Decisions were made to protect individual identity by deleting names, eliminating day of birth and race as data elements, and removing the encrypted patient identifier once that data was received and edited by the State's data base staff following which a new random number would be assigned. This provided an extra layer of protection to ensure individual patient confidentiality. While consideration was given to requiring informed consent before information could be submitted to the statewide database this was considered unnecessary given the anonymity of the data. This point is still under debate at the state level.

Data Access

With regard to data stored in a statewide comprehensive medical database, access, authorization and authentication were considered. This involved consideration of policy decisions regarding who has a right to view the information, how access is granted and how authorized users are verified. While it was acknowledged that access to specific components of information could be controlled through encryption and digital signature in conjunction with policies, use of encryption was also viewed as a factor which could double or triple the cost of the system.

Given these factors and the decision to strip identifiers from the data, the need to protect sensitive data became less of an issue. Still, policy was necessary to identify the types of public-use data to be developed for legitimate academic research and for third party access to data sets other than the public-use data sets.

Protection of Proprietary Information

Utilization assumptions and physician fee schedules that are used to develop reimbursement rates are considered confidential commercial information, and, as such, are not publicly disclosed. Similarly, capitation rates are considered confidential because they are population specific; cover a wide range of services and may not allow for fair comparisons to be made. For example, without careful risk adjustment, payers and providers that cover the more sick populations could be unfairly portrayed.

The Public Information Act of Maryland[4] recognizes that the release of certain information could cause harm to the competitive position of the original source (payer and provider). In public debate, payers considered aggregate data to be proprietary because the information allows for uniform comparisons, such as between hospitals or providers. No specific recommendation was developed on this issue although it was decided that practitioner identifiers, would be assigned a specialty designation and given an encrypted identifier by the data management contractor.

Development of Public Use Data

The rationale for making public use data available is to place more information into the hands of health care consumers. It is assumed that greater access to information about where and how health care dollars are being spent will help both policy-makers and health care purchasers make wiser decisions.

Decisions were made that data released in the public use files would not include the medical record number, physician identifier, birth date or date of admission or discharge. There is a procedure by which length of stay is derived to replace actual dates of service. Release of information beyond that in public research files was required to be reviewed on a case-by-case basis to ensure that data requested would support legitimate research and that appropriate controls would be established to limit access and release.

Recommendations were made that specific payer names and identifiers be excluded from any public research data set and that the data set include more general payer information to support comparisons of different delivery systems. Also recommended was that the public research data set exclude physician names and unique identifiers but contain information on physician specialty and practice type. Before releasing any public-use data, it was recommended that there be a careful examination of the public release data to ensure that accidental disclosure could not occur because of small cell sizes.

Third Party Access to Other than Public-Use

Data Sets
Procedures for release of data for research centered on establishing an information review board representative of the interest groups

that had participated in the public debates to advise staff prior to the release of data. Protocols must define: who can request data; acceptable types of requests; and the establishment of security procedures that include prohibiting any requesting organization from secondary release of detailed information.

CONCLUSIONS

Construction of data release policies for the Federal Government and States is an essential component of public database collection and analysis. It is critical that this occur in a public forum that includes consumers, providers, payers and regulators. Divergent views regarding the appropriateness, utility and benefit or harm represented by health care databases in the public arena can shape not only the policy that regulates practice but also, consumer health care decisions.

Databases must meet consumer and policy needs to support the development of payment systems, assessment of insurance reform, examination of access to care, identification of cost differences, and expansion of information to the consumer. The policy guiding the collection, development and use of this data must be created around core issues of confidentiality and security.

References

1. Whelan v. Roe, 429 U.S. 589, 599 (1977).
2. Dr. K. v State Board, 98 Md. App. 103, 112 (1994).
3. Harris/Equifax Health Care Privacy Survey. 1993. Columbia University. New York.
4. Maryland State Government Article #10-617(b).